

DOCKET NO. 2000.04.017.WT0

Customer No. 23990

1 Km AF/2135  
PATENT



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Re application of : Bryan J. Moles, et al.  
Serial No. : 09/475,602  
Filed : December 30, 1999  
For : SYSTEM AND METHOD FOR SECURE PROVISIONING OF  
A MOBILE STATION FROM A PROVISIONING SERVER  
USING IP ADDRESS TRANSLATION AT THE BTS/BSC  
Art Unit : 2135  
Examiner : Beemnet W. Dada

**MAIL STOP APPEAL BRIEF - PATENTS**

Commissioner of Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**CERTIFICATE OF MAILING BY FIRST CLASS MAIL**

Sir:

The undersigned hereby certifies that the following documents:

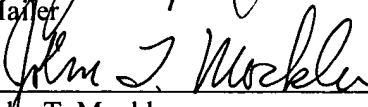
1. Postcard Receipt;
2. Appellants' Brief on Appeal;
3. Fee Transmittal FY 2008 (in duplicate); and
4. Check in the amount of \$510.00 for Appeal Brief filing fee

relating to the above application, were deposited as "First Class Mail" with the United States Postal Service, addressed to MAIL STOP APPEAL BRIEF - PATENTS, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on **June 6, 2008**.

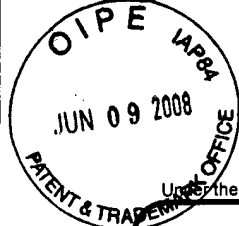
Date: June 6, 2008

  
\_\_\_\_\_  
Mailer

Date: June 6, 2008

  
\_\_\_\_\_  
John T. Mockler  
Reg. No. 39,775

P.O. Drawer 800889  
Dallas, Texas 75380  
Phone: (972) 628-3600  
Fax: (972) 628-3616  
E-mail: [jmockler@munckcarter.com](mailto:jmockler@munckcarter.com)



PTO/SB/17 (10-07)

Approved for use through 06/30/2010. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 12/08/2004.

Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

# FEE TRANSMITTAL

## For FY 2008

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT (\$) 510.00

**Complete if Known**

Application Number	09/475,602
Filing Date	December 30, 1999
First Named Inventor	Bryan J. Moles
Examiner Name	Beemnet W. Dada
Art Unit	2135
Attorney Docket No.	SAMS01-00097

**METHOD OF PAYMENT** (check all that apply)☒ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): \_\_\_\_\_☒ Deposit Account Deposit Account Number: 50-0208 Deposit Account Name: Munck Carter, P.C.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**☒ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

**FEE CALCULATION****1. BASIC FILING, SEARCH, AND EXAMINATION FEES**

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
Utility	310	155	510	255	210	105	
Design	210	105	100	50	130	65	
Plant	210	105	310	155	160	80	
Reissue	310	155	510	255	620	310	
Provisional	210	105	0	0	0	0	

**2. EXCESS CLAIM FEES****Fee Description**

Each claim over 20 (including Reissues)

Each independent claim over 3 (including Reissues)

Multiple dependent claims

Fee (\$)	Small Entity Fee (\$)
50	25
210	105
370	185

**Total Claims** **Extra Claims** **Fee (\$)** **Fee Paid (\$)**

- 20 or HP = \_\_\_\_\_ x \_\_\_\_\_ = \_\_\_\_\_

HP = highest number of total claims paid for, if greater than 20.

**Indep. Claims** **Extra Claims** **Fee (\$)** **Fee Paid (\$)**

- 3 or HP = \_\_\_\_\_ x \_\_\_\_\_ = \_\_\_\_\_

HP = highest number of independent claims paid for, if greater than 3.

**3. APPLICATION SIZE FEE**

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is \$260 (\$130 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

<b>Total Sheets</b>	<b>Extra Sheets</b>	<b>Number of each additional 50 or fraction thereof</b>	<b>Fee (\$)</b>	<b>Fee Paid (\$)</b>
_____ - 100 = _____	_____ / 50 = _____	(round up to a whole number) x _____	= _____	

**4. OTHER FEE(S)**

Non-English Specification, \$130 fee (no small entity discount)

Other (e.g., late filing surcharge): Appeal Brief**Fees Paid (\$)**

\$510.00

**SUBMITTED BY**

Signature	<u>John T. Mockler</u>	Registration No. (Attorney/Agent) 39,775	Telephone 972-628-3600
Name (Print/Type)	John T. Mockler		Date June 6, 2008

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



DUPLICATE

PTO/SB/17 (10-07)

Approved for use through 06/30/2010. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 12/08/2004.

Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

**FEE TRANSMITTAL**  
**For FY 2008**☐ Applicant claims small entity status. See 37 CFR 1.27TOTAL AMOUNT OF PAYMENT (\$)  
510.00**Complete if Known**

Application Number	09/475,602
Filing Date	December 30, 1999
First Named Inventor	Bryan J. Moles
Examiner Name	Beemnet W. Dada
Art Unit	2135
Attorney Docket No.	SAMS01-00097

**METHOD OF PAYMENT** (check all that apply)☒ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): \_\_\_\_\_☒ Deposit Account Deposit Account Number: 50-0208 Deposit Account Name: Munck Carter, P.C.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee☒ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

**FEE CALCULATION****1. BASIC FILING, SEARCH, AND EXAMINATION FEES**

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
Utility	310	155	510	255	210	105	
Design	210	105	100	50	130	65	
Plant	210	105	310	155	160	80	
Reissue	310	155	510	255	620	310	
Provisional	210	105	0	0	0	0	

**2. EXCESS CLAIM FEES**

Fee Description	Fee (\$)	Small Entity Fee (\$)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	210	105
Multiple dependent claims	370	185
<b>Total Claims</b>	<b>Extra Claims</b>	<b>Fee (\$)</b>
- 20 or HP = _____ x _____ = _____		
HP = highest number of total claims paid for, if greater than 20.		
<b>Indep. Claims</b>	<b>Extra Claims</b>	<b>Fee (\$)</b>
- 3 or HP = _____ x _____ = _____		
HP = highest number of independent claims paid for, if greater than 3.		

**3. APPLICATION SIZE FEE**

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is \$260 (\$130 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee (\$)	Fees Paid (\$)
- 100 = _____	/ 50 = _____	(round up to a whole number) x _____	= _____	

**4. OTHER FEE(S)**

Non-English Specification, \$130 fee (no small entity discount)

Other (e.g., late filing surcharge): Appeal Brief

Fees Paid (\$)

\$510.00

**SUBMITTED BY**

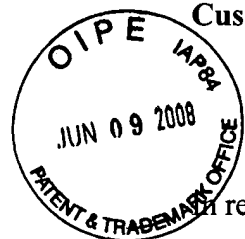
Signature	<u>John T. Mockler</u>	Registration No. (Attorney/Agent)	39,775	Telephone	972-628-3600
Name (Print/Type)	John T. Mockler			Date	June 6, 2008

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

DOCKET NO. 2000.04.017.WT0  
Customer No. 23990

PATENT



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

re application of : Bryan J. Moles, et al.  
Serial No. : 09/475,602  
Filed : December 30, 1999  
For : SYSTEM AND METHOD FOR SECURE PROVISIONING OF A  
MOBILE STATION FROM A PROVISIONING SERVER USING  
IP ADDRESS TRANSLATION AT THE BTS/BSC  
Art Unit : 2135  
Examiner : Beemnet W. Dada

**MAIL STOP APPEAL BRIEF - PATENTS**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

**APPELLANTS' BRIEF ON APPEAL**

Appellant respectfully submits that the Examiner's decision of December 31, 2007, finally rejecting Claims 1-20 in the present application, should be reversed, in view of the following arguments and authorities. This Appeal Brief is submitted on behalf of Appellants for the above-identified application. A Notice of Appeal was filed on March 31, 2008, and received in the Patent Office on April 4, 2008. A Pre-Appeal Brief Request for Review was filed along with the Notice of Appeal. A Pre-Appeal Brief conference determined that there is at least one actual issue for appeal and the application remains under appeal.

**REAL PARTY IN INTEREST**

The real party in interest for this appeal is the assignee of the application, Samsung Electronics Co., Ltd.

**RELATED APPEALS AND INTERFERENCES**

There are no other appeals or interferences related to the present application that are currently pending

**STATUS OF CLAIMS**

Claims 1-20 were originally filed and remain pending in the application. Claims 1-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,587,684 to *Hsu, et al.* in view of U. S. Patent No. 6,321,336 to *Applegate, et al.* Claims 1-20 are presented for appeal. A copy of all pending claims is provided in Appendix A.

**STATUS OF AMENDMENTS**

No claims were amended after final rejection.



**SUMMARY OF CLAIMED SUBJECT MATTER**

Regarding Claim 1, a security device is recited, for use in a wireless network that comprises a plurality of base stations, each of the base stations capable of communicating with a plurality of mobile stations. *See Specification, Fig. 1, page 14, lines 10-19.* The security device is capable of preventing an unprovisioned one of the plurality of mobile stations from accessing an Internet protocol (IP) data network through the wireless network. *See Specification, Fig. 3, page 21, lines 14-22.* The security device includes a first controller that is capable of receiving from the unprovisioned mobile station an IP data packet comprising an IP packet header and an IP packet payload. *See Specification, Fig. 4, page 25, lines 12-20.* The first controller is also capable of replacing the IP packet header with a replacement IP packet header comprising an IP address of a selected one of a plurality of provisioning servers that are associated with the wireless network. *Id.*

Regarding Claim 9, a wireless network includes a plurality of base stations (each capable of communicating with a plurality of mobile stations), at least one provisioning server, and a security device. *See Specification, Fig. 1, page 14, lines 10-19, and Fig. 3, page 21, lines 14-22.* The security device is capable of preventing an unprovisioned one of the plurality of mobile stations from accessing an Internet protocol (IP) data network through the wireless network. *See Specification, Fig. 3, page 21, lines 14-22.* The security device includes a first controller that is capable of receiving from the unprovisioned mobile station an IP data packet comprising an IP packet header and an IP packet payload. *See Specification, Fig. 4, page 25, lines 12-20.* The first controller is also capable of replacing the IP packet header with a replacement IP packet header comprising an IP

address of a selected one of a plurality of provisioning servers that are associated with the wireless network. *Id.* In this way, the security device is capable of preventing the unprovisioned mobile station from accessing the Internet protocol (IP) data network through the wireless network by addressing IP packets from the mobile station to the selected provisioning server.

Regarding Claim 17, a method is recited for use in a wireless network that comprises a plurality of base stations, each of the base stations capable of communicating with a plurality of mobile stations. *See Specification, Fig. 1, page 14, lines 10-19.* The method of preventing an unprovisioned one of the plurality of mobile stations from accessing an Internet protocol (IP) data network through the wireless network includes receiving from the unprovisioned mobile station an IP data packet comprising an IP packet header and an IP packet payload. *See Specification, Fig. 4, page 25, lines 12-20.* The method also includes determining that the unprovisioned mobile station is unprovisioned. *See Specification, Fig. 5, page 29, line 17, through page 30, line 2.* The method further includes replacing the IP packet header with a replacement IP packet header comprising an IP address of a selected one of a plurality of provisioning servers associated with the wireless network. *See Specification, Fig. 5, page 30, lines 5-10.* In this way, the method prevents the unprovisioned mobile station from accessing the Internet protocol (IP) data network through the wireless network by addressing IP packets from the mobile station to the selected provisioning server.

**GROUND OF REJECTION TO BE REVIEWED UPON APPEAL**

1. Claims 1-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,587,684 to *Hsu, et al.* in view of U. S. Patent No. 6,321,336 to *Applegate, et al.*

**ARGUMENT**

**I. GROUND OF REJECTION #1 (§ 103 REJECTION)**

The rejection of Claims 1-20 under 35 U.S.C. § 103(a) is improper and should be withdrawn.

**A. OVERVIEW**

Claims 1-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,587,684 to *Hsu, et al.* (hereinafter, “Hsu”) in view of U. S. Patent No. 6,321,336 to *Applegate, et al.* (hereinafter, “Applegate”).

**B. STANDARD**

**35 U.S.C. § 103**

In rejecting claims under 35 U.S.C. § 103(a), the examiner bears the initial burden of establishing a *prima facie* case of obviousness. (*In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). See also *In re Piasecki*, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984)). It is incumbent upon the examiner to establish a factual basis to support the legal conclusion of obviousness. (*Id.* at 1073, 5 USPQ2d at 1598). In so doing, the examiner is expected to make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (1966), viz., (1) the scope and content of the prior art; (2) the differences between the prior art and the claims at issue; and (3) the level of ordinary skill in the art. In addition to these factual determinations, the examiner must also provide “some articulated reasoning with some

rational underpinning to support the legal conclusion of obviousness.” (*In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir 2006) (cited with approval in *KSR Int’l v. Teleflex Inc.*, 127 S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007)).

### **Considering the Invention as a Whole**

When applying 35 U.S.C. 103, the claimed invention must be considered as a whole. *See MPEP § 2141(II)*. In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *MPEP § 2141.02(I)*, citing *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983). Indeed, The Supreme Court has recently held,

[A] patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. Although common sense directs one to look with care at a patent application that claims as innovation the combination of two known devices according to their established functions, it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. *KSR Intern. Co. v. Teleflex Inc.*, 127 S.Ct. 1727 (U.S.,2007).

### **Solving a Problem Already Solved**

In *Ex Parte Rinkevich et al.* (BPAI 2007-1317, non-precedential), the BPAI applies KSR to reason that a skilled person would not look to a second patent to solve a problem already solved by a first patent (and by the patentee). The BPAI wrote: "In the instant case, we conclude that a person of ordinary skill in the art having common sense at the time of the invention would not have reasonably

looked to Wu to solve a problem already solved by Savill. Therefore, we agree with Appellants that the Examiner has impermissibly used the instant claims as a guide or roadmap in formulating the rejection."

See <http://des.uspto.gov/Foia/ReterivePdf?system=BPAI&flNm=fd2007131705-29-2007>

### **Fully and Clearly Stated Grounds of Rejection**

A proper rejection must be stated clearly and specifically. MPEP § 707.07(d), page 700-125 (8th ed. rev. 6, September 2007) ("Where a claim is refused for any reason relating to the merits thereof it should be 'rejected' and the ground of rejection fully and clearly stated..."") (*Emphasis added*).

As further clarified in MPEP § 2142:

The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. \_\_\_, \_\_\_, 82 USPQ2d 1385, 1396 (2007) noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements"; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006). See also *KSR*, 550 U.S. at \_\_\_, 82 USPQ2d at 1396 (quoting Federal Circuit statement with approval). *MPEP § 2142, pages 2100-127 through 2100-128 (8th ed. rev. 6, September 2007) (Emphasis added).*

### **C. THE HSU REFERENCE**

The Hsu reference provides an over-the-air cellphone provisioning procedure. *See Hsu, col. 14, lines 13-18.* In an initial step, the purchaser of a digital telephone calls a customer service center

using a predetermined phone number. *See Hsu, col. 14, lines 19-26.* The customer service center receives user identity and credit-related information from the purchaser, establishes an account for the purchaser, and activates the account. *See Hsu, col. 14, lines 31-48.* The purchaser then initiates an activation routine that makes a wireless data call to an interworking function (IWF), which assigns the digital telephone a temporary IP address and provides the IP address of a data proxy server/gateway. *See Hsu, col. 14, line 49, through col. 15, line 6.* The telephone establishes a link with the proxy server and receives a uniform resource locator (URL) for the sole provisioning server in the system of Hsu. *See Hsu, col. 15, lines 24-29.* The telephone uses the URL provided to it by the proxy server to communicate with the provisioning server in completing the provisioning procedure. *See Hsu, col. 15, lines 30-50.*

**D. THE APPLGATE REFERENCE**

The Applegate reference describes a firewall for securing traffic between an internal network and an external network. *See Applegate, col. 2, lines 43-46.* The firewall receives a message from a host on the internal network, the message including a destination address. *See Applegate, col. 2, lines 11-13.* The firewall saves the original destination address and replaces it with the address of an FTP proxy within the firewall. *See Applegate, col. 5, lines 24-30.* The FTP proxy receives the redirected message, examines the original destination address, and if communication with that address is allowed, replaces the FTP proxy address with the original address and sends the message to the external network. *See Applegate, col. 5, lines 55-64.*

**E. CLAIM 1**

Claim 1 recites

[f]or use in a wireless network comprising a plurality of base stations, each of said base stations capable of communicating with a plurality of mobile stations, a security device capable of preventing an unprovisioned one of said plurality of mobile stations from accessing an Internet protocol (IP) data network through said wireless network, said security device comprising:

a first controller capable of receiving from said unprovisioned mobile station an IP data packet comprising an IP packet header and an IP packet payload and replacing said IP packet header with a replacement IP packet header comprising an IP address of a selected one of a plurality of provisioning servers associated with said wireless network.

First, Examiner Dada acknowledges that Hsu does not describe a controller that receives an IP data packet and replaces the received IP packet header with an IP packet header including an IP address of a selected one of a plurality of provisioning servers. But, Examiner Dada asserts that replacing an IP header with the IP address of a server is well-known in the art, “in order to route data to a correct destination address and further provide efficient data transmission.” *See final Office Action, mailed December 31, 2007, sentence beginning last line of page 3.*

However, routing data to a correct destination address and providing efficient data transmission are problems that Hsu has already solved. Hsu ensures that provisioning messages go only to the provisioning server by providing the server’s address to a wireless device for its use during provisioning. As such Hsu has provided a mechanism for routing data to a correct destination address and providing efficient data transmission. Examiner Dada has provided no explanation why a person of ordinary skill in the art having common sense at the time of the invention would have



reasonably looked to Applegate to solve a problem already solved by Hsu. Instead, the Appellants respectfully submit that Examiner Dada has impermissibly used Claim 1 as a guide in formulating the rejection.

Second, in further support of the assertion that replacing an IP header with the IP address of a server is well-known in the art, Examiner Dada cites Applegate. The Examiner asserts that Applegate describes replacing an IP packet header with a replacement IP packet header including the IP address of a selected one of a plurality of servers associated with a wireless network, citing column 5, lines 34-65. The Applicants respectfully submit that Examiner Dada appears to mischaracterize several aspects of the Applegate reference.

Applegate describes a firewall that reroutes an FTP packet to a local FTP proxy by replacing the IP address of an external FTP server with the IP address of the FTP proxy. However, Applegate makes no mention of a plurality of FTP proxies, nor of selecting one proxy from a plurality of proxies. Also, Applegate describes a communication security system that uses a server to communicate to an unprotected network, such as the Internet, but Applegate makes no mention of a wireless network. Furthermore, Examiner Dada asserts that a person of skill in the art would turn to the teaching of Applegate in order to efficiently route packets and further enhance security of the system. Applegate provides no suggestion that replacing the IP address of an FTP server with the address of an FTP proxy provides efficient routing of packets, and the security enhancements of Applegate come not from replacing the IP address in the FTP packet, but rather from checking in the FTP proxy whether a connection to the intended FTP server is permitted.

In short, Examiner Dada has suggested that a person of skill in the art would combine Hsu and Applegate to solve a problem that does not exist in Hsu with a feature of Applegate that does not provide the improvement that the Examiner suggests. The suggestion that the security of over-the-air provisioning should be improved and the solution of replacing the IP address in a data packet from an unprovisioned mobile station with the IP address of a provisioning server come only from the present application, not from the cited references.

Third, while Hsu describes a proxy gateway sending the URL of a provisioning server to a wireless device, Hsu describes only a single provisioning server, not a plurality of provisioning servers, as asserted by Examiner Dada.

As such, Examiner Dada has not shown that the cited references teach or suggest all the limitations of Claim 1. For these reasons, the Examiner has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 1 under § 103 be withdrawn and that Claim 1 be passed to allowance.

**F. CLAIM 2**

Claim 2 recites the security device of Claim 1, wherein the first controller is disposed in at least one of the plurality of base stations.

As Claim 2 depends from Claim 1, the arguments above with regard to the patentability of Claim 1 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 1, Examiner Dada interpreted the proxy server of Hsu as teaching the recited first controller. *See final Office Action, mailed December 31, 2007, page 3, section 5, second paragraph, first sentence.* In rejecting Claim 2, Examiner Dada stated that Hsu further teaches that the first controller is disposed in at least one of the plurality of base stations at column 6, lines 25-30. *See final Office Action, page 5, section 7.* The cited passage is reproduced below:

Specifically, the IWF 18 provides an interworking function, where data packets transmitted by a digital telephone 16 and received by the BSC 14 are routed to the IWF 18 via the MSC 12 based on dialed digits supplied from the digital telephone 16.

The Appellants note that the cited passage makes no reference at all to the proxy server that Examiner Dada asserted describes the recited first controller. Furthermore, the Appellants are unable to find in the cited passage (or any other part of Hsu) any description of the proxy server of Hsu being disposed in the base station of Hsu.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 2 under § 103 be withdrawn and that Claim 2 be passed to allowance.

**G. CLAIM 3**

Claim 3 recites the security device of Claim 1, wherein the first controller is disposed in a mobile switching center of the wireless network.

As Claim 3 depends from Claim 1, the arguments above with regard to the patentability of Claim 1 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 1, Examiner Dada interpreted the proxy server of Hsu as teaching the recited first controller. *See final Office Action, mailed December 31, 2007, page 3, section 5, second paragraph, first sentence.* In rejecting Claim 3, Examiner Dada stated that Hsu further teaches that the first controller is disposed in at least one of the plurality of base stations at column 6, lines 25-30. *See final Office Action, page 5, section 8.* The cited passage is reproduced below:

Specifically, the IWF 18 provides an interworking function, where data packets transmitted by a digital telephone 16 and received by the BSC 14 are routed to the IWF 18 via the MSC 12 based on dialed digits supplied from the digital telephone 16.

The Appellants note that the cited passage makes no reference at all to the proxy server that Examiner Dada asserted describes the recited first controller. Furthermore, the Appellants are unable to find in the cited passage (or any other part of Hsu) any description of the proxy server of Hsu being disposed in the mobile switching center of Hsu.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 3 under § 103 be withdrawn and that Claim 3 be passed to allowance.

#### **H. CLAIM 4**

Claim 4 recites the security device of Claim 1, further comprising a second controller capable of determining that said unprovisioned mobile station is unprovisioned.

As Claim 4 depends from Claim 1, the arguments above with regard to the patentability of Claim 1 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 4, Examiner Dada makes the conclusory statement, "As per claim [4], Hsu further teaches determining the unprovisioned mobile stations is (sic) unprovisioned (column 15, lines 7-10 and 21-25)." *Final Office Action, mailed December 31, 2007, page 5, section 9.*

Initially, the Appellants note that Examiner Dada has failed even to assert that Hsu or Applegate describes or suggests a second controller. As such, the Examiner has failed to establish a *prima facie* case of obviousness by failing to show that the prior art teaches or suggests all the elements of the claim.

The cited passages state:

As shown in FIG. 4B , the digital telephone 16 then establishes an initial two-way application session 62 with the proxy server 20 in step 128 . The digital telephone 16 also sends a data activation request with a security key and an international mobile station identity (IMSI). *Hsu, col. 15, lines 7-11.*

The proxy gateway 20 will also access the database [28] to determine if the user is in the active mode, indicating that the subscriber is already activated. If the user is not in an active mode, the proxy server 20 accepts the provisioning request in step 134 by transmitting a uniform resource locator (URL) to the digital telephone 16 and initiates a secure link using the user authenticated code and a public key encryption algorithm, such as the Diffie-Hellman algorithm. *Hsu, col. 15, lines 21-29. Reference character typo corrected.*

In rejecting Claim 1, Examiner Dada interpreted the proxy server of Hsu as teaching the recited first controller. *See final Office Action, mailed December 31, 2007, page 3, section 5, second paragraph, first sentence.* The passages cited in rejecting Claim 4 provide further description of the proxy server and, therefore, do not describe the second controller recited in Claim 4.

As such, the Appellants submit that Examiner Dada has failed to fully and clearly state the grounds for rejecting Claim 4. Specifically, the Examiner has not shown where Hsu describes the

recited second controller capable of determining that an unprovisioned mobile station is unprovisioned.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 4 under § 103 be withdrawn and that Claim 4 be passed to allowance.

**I. CLAIM 5**

Claim 5 recites the security device of Claim 4, wherein the second controller determines that the unprovisioned mobile station is unprovisioned if the unprovisioned mobile station is unable to authenticate to the wireless network.

As Claim 5 depends from Claim 4, the arguments above with regard to the patentability of Claim 4 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 5, Examiner Dada makes the conclusory statement, “As per claim [5], Hsu further teaches determining the unprovisioned mobile stations is (sic) unprovisioned (column 15, lines 7-10 and 21-25).” *Final Office Action, mailed December 31, 2007, page 5, section 9.*

Initially, the Appellants note that Examiner Dada has failed even to assert that Hsu or Applegate describes or suggests determining that a mobile station is unprovisioned from the inability of the mobile station to authenticate to a wireless network. As such, the Examiner has failed to establish a *prima facie* case of obviousness by failing to show that the prior art teaches or suggests all the elements of the claim.

The cited passages state:

As shown in FIG. 4B , the digital telephone 16 then establishes an initial two-way application session 62 with the proxy server 20 in step 128 . The digital telephone 16 also sends a data activation request with a security key and an international mobile station identity (IMSI). *Hsu, col. 15, lines 7-11.*

The proxy gateway 20 will also access the database [28] to determine if the user is in the active mode, indicating that the subscriber is already activated. If the user is not in an active mode, the proxy server 20 accepts the provisioning request in step 134 by transmitting a uniform resource locator (URL) to the digital telephone 16 and initiates a secure link using the user authenticated code and a public key encryption algorithm, such as the Diffie-Hellman algorithm. *Hsu, col. 15, lines 21-29. Reference character typo corrected.*

The Appellants are unable to find in the cited passages any teaching or suggestion of a mobile station authenticating to a wireless network, much less determining that a mobile station is unprovisioned from its inability to authenticate to the network.

As such, the Appellants submit that Examiner Dada has failed to fully and clearly state the grounds for rejecting Claim 5. Specifically, the Examiner has not shown where Hsu describes the recited second controller capable of determining that an unprovisioned mobile station is unprovisioned if the mobile station is unable to authenticate to the wireless network.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 5 under § 103 be withdrawn and that Claim 5 be passed to allowance.

**J. CLAIM 6**

Claim 6 recites the security device of Claim 4, wherein the second controller determines that the unprovisioned mobile station is unprovisioned according to a predetermined telephone number associated with a service provisioning process selected by the unprovisioned mobile station.

As Claim 6 depends from Claim 4, the arguments above with regard to the patentability of Claim 4 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 6, Examiner Dada makes the conclusory statement, “As per claim [6], Hsu further teaches determining the unprovisioned mobile stations is (sic) unprovisioned (column 15, lines 7-10 and 21-25).” *Final Office Action, mailed December 31, 2007, page 5, section 9.*

Initially, the Appellants note that Examiner Dada has failed even to assert that Hsu or Applegate describes or suggests determining that a mobile station is unprovisioned according to a predetermined telephone number associated with a service provisioning process selected by the unprovisioned mobile station. As such, the Examiner has failed to establish a *prima facie* case of obviousness by failing to show that the prior art teaches or suggests all the elements of the claim.

The cited passages state:

As shown in FIG. 4B , the digital telephone 16 then establishes an initial two-way application session 62 with the proxy server 20 in step 128 . The digital telephone 16 also sends a data activation request with a security key and an international mobile station identity (IMSI). *Hsu, col. 15, lines 7-11.*

The proxy gateway 20 will also access the database [28] to determine if the user is in the active mode, indicating that the subscriber is already activated. If the user is not in an active mode, the proxy server 20 accepts the provisioning request in step 134 by transmitting a uniform resource locator (URL) to the digital telephone 16 and initiates a secure link using the user authenticated code and a public key encryption



algorithm, such as the Diffie-Hellman algorithm. *Hsu, col. 15, lines 21-29. Reference character typo corrected.*

The Appellants are unable to find in the cited passages any teaching or suggestion of predetermined telephone numbers associated with a service provisioning process, or an unprovisioned mobile station selecting a service provisioning process, much less determining that a mobile station is unprovisioned according to a predetermined telephone number associated with a service provisioning process selected by the unprovisioned mobile station

As such, the Appellants submit that Examiner Dada has failed to fully and clearly state the grounds for rejecting Claim 6. Specifically, the Examiner has not shown where Hsu describes the recited second controller capable of determining that an unprovisioned mobile station is unprovisioned according to a predetermined telephone number associated with a service provisioning process selected by the unprovisioned mobile station.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 6 under § 103 be withdrawn and that Claim 6 be passed to allowance.

**K. CLAIM 7**

Claim 7 recites the security device of Claim 4, wherein the second controller determines that the unprovisioned mobile station is unprovisioned according to data retrieved from a home location register associated with said wireless network.

As Claim 7 depends from Claim 4, the arguments above with regard to the patentability of Claim 4 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 7, Examiner Dada makes the conclusory statement, "As per claim [7], Hsu further teaches determining the unprovisioned mobile stations is (sic) unprovisioned (column 15, lines 7-10 and 21-25)." *Final Office Action, mailed December 31, 2007, page 5, section 9.*

Initially, the Appellants note that Examiner Dada has failed even to assert that Hsu or Applegate describes or suggests determining that a mobile station is unprovisioned according to data retrieved from a home location register associated with said wireless network. As such, the Examiner has failed to establish a *prima facie* case of obviousness by failing to show that the prior art teaches or suggests all the elements of the claim.

The cited passages state:

As shown in FIG. 4B , the digital telephone 16 then establishes an initial two-way application session 62 with the proxy server 20 in step 128 . The digital telephone 16 also sends a data activation request with a security key and an international mobile station identity (IMSI). *Hsu, col. 15, lines 7-11.*

The proxy gateway 20 will also access the database [28] to determine if the user is in the active mode, indicating that the subscriber is already activated. If the user is not in an active mode, the proxy server 20 accepts the provisioning request in step 134 by transmitting a uniform resource locator (URL) to the digital telephone 16 and initiates a secure link using the user authenticated code and a public key encryption algorithm, such as the Diffie-Hellman algorithm. *Hsu, col. 15, lines 21-29. Reference character typo corrected.*

The Appellants are unable to find in the cited passages any teaching or suggestion of determining that a mobile station is unprovisioned according to data retrieved from a home location register associated with said wireless network.

The user database 28 described in the cited passages stores an international mobile station identify (IMSI), a security key, and an 'active' status mode indication. *See Hsu, col. 15, lines 13-29, and Claims 6, 24 and 33.* The user database 28 is clearly not a home location register.

In fact, Hsu describes a home location register as separate from the user database 28. The home location register is part of operation maintenance provisioning system 44. *See Hsu, Fig. 1, col. 7, lines 50-59.*

As such, the Appellants submit that Examiner Dada has failed to fully and clearly state the grounds for rejecting Claim 7. Specifically, the Examiner has not shown where Hsu describes the recited second controller capable of determining that an unprovisioned mobile station is unprovisioned according to data retrieved from a home location register associated with said wireless network.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 7 under § 103 be withdrawn and that Claim 7 be passed to allowance.

**L.     CLAIM 8**

Claim 8 recites the security device of Claim 1, wherein the first controller selects the at least one provisioning server by selecting said IP address in said replacement IP packet header according to a load spreading algorithm.

As Claim 8 depends from Claim 1, the arguments above with regard to the patentability of Claim 1 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 8, Examiner Dada stated that Applegate describes selecting an IP address according to a load sharing algorithm in column 5, lines 34-65. *See final Office Action, mailed December 31, 2007, page 5, section 10.* The Appellants respectfully submit that Examiner Dada appears to mischaracterize the teaching of the Applegate reference.

The cited passage is reproduced below:

The message packet is then passed along 366 to TCP/IP 226. The modified message packet has: source IP address 199.198.10.2, source port 1024, destination IP address 199.198.10.1, and destination port 21. The IP layer then examines the IP header, determines that the message is destined for the Firewall machine and accepts it. TCP/IP passes the message along to the FTP proxy, which is listening for incoming messages. The FTP proxy 310 obtains the message, verifies that the FTP connection is permitted by an access control entry, and hides the internal source of the message from the external network. *Applegate, col. 5, lines 34-64*

There is clearly no description in the cited passage of selecting an IP address according to a load sharing algorithm, as asserted by Examiner Dada. In fact, Applegate describes a firewall that reroutes an FTP packet to a local FTP proxy by replacing the IP address of an external FTP server with the IP address of the FTP proxy. There is only a single FTP proxy in Applegate, therefore Applegate cannot teach selecting one of a plurality of servers, much less selecting a server according to a load sharing algorithm.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 8 under § 103 be withdrawn and that Claim 8 be passed to allowance.

**M. CLAIM 9**

Claim 9 recites a wireless network comprising:

- a plurality of base stations, each of said base stations capable of communicating with a plurality of mobile stations;
- at least one provisioning server; and
- a security device capable of preventing an unprovisioned one of said plurality of mobile stations from accessing an Internet protocol (IP) data network through said wireless network, said security device comprising:
  - a first controller capable of receiving from said unprovisioned mobile station an IP data packet comprising an IP packet header and an IP packet payload and replacing said IP packet header with a replacement IP packet header comprising an IP address of said provisioning server.

First, Examiner Dada acknowledges that Hsu describes transmitting a URL of a provisioning server to a wireless device, rather than describing replacing a received IP packet header with an IP packet header including an IP address of a selected one of a plurality of provisioning servers. But, Examiner Dada asserts that replacing an IP header with the IP address of a server is well-known in the art, “in order to route data to a correct destination address and further provide efficient data transmission.” *See final Office Action, mailed December 31, 2007, sentence beginning last line of page 4.*

Routing data to a correct destination address and providing efficient data transmission, the motivations proposed by Examiner Dada, are problems that Hsu has already solved. Hsu ensures that provisioning messages go only to the provisioning server by providing the server’s address to a wireless device for its use during provisioning, as acknowledged by the Examiner. As such Hsu has already provided a mechanism for routing data to a correct destination address and providing

efficient data transmission. Examiner Dada has provided no explanation why a person of ordinary skill in the art having common sense at the time of the invention would have reasonably looked to Applegate to solve a problem already solved by Hsu. Instead, the Appellants respectfully submit that Examiner Dada has impermissibly used Claim 1 as a guide in formulating the rejection.

Second, in further support of the assertion that replacing an IP header with the IP address of a server is well-known in the art, Examiner Dada cites Applegate. The Examiner asserts that Applegate describes replacing an IP packet header with a replacement IP packet header including the IP address of a selected one of a plurality of servers associated with a wireless network, citing column 5, lines 34-65. The Applicants respectfully submit that Examiner Dada appears to mischaracterize several aspects of the Applegate reference.

Applegate describes a firewall that reroutes an FTP packet to a local FTP proxy by replacing the IP address of an external FTP server with the IP address of the FTP proxy. However, Applegate makes no mention of a plurality of FTP proxies, nor of selecting one proxy from a plurality of proxies. Also, Applegate describes a communication security system that uses a server to communicate to an unprotected network, such as the Internet, but Applegate makes no mention of a wireless network. Furthermore, Examiner Dada asserts that a person of skill in the art would turn to the teaching of Applegate in order to efficiently route packets and further enhance security of the system. Applegate provides no suggestion that replacing the IP address of an FTP server with the address of an FTP proxy provides efficient routing of packets, and the security enhancements of

Applegate come not from replacing the IP address in the FTP packet, but rather from checking in the FTP proxy whether a connection to the intended FTP server is permitted.

In short, Examiner Dada has suggested that a person of skill in the art would combine Hsu and Applegate to solve a problem that does not exist in Hsu with a feature of Applegate that does not provide the improvement that the Examiner suggests. The suggestion that the security of over-the-air provisioning should be improved and the solution of replacing the IP address in a data packet from an unprovisioned mobile station with the IP address of a provisioning server come only from the present application, not from the cited references.

Third, while Hsu describes a proxy gateway sending the URL of a provisioning server to a wireless device, Hsu describes only a single provisioning server, not a plurality of provisioning servers, as asserted by Examiner Dada.

As such, Examiner Dada has not shown that the cited references teach or suggest all the limitations of Claim 1. For these reasons, the Examiner has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 1 under § 103 be withdrawn and that Claim 1 be passed to allowance.

N. **CLAIM 10**

Claim 10 recites the wireless network of Claim 9, wherein the first controller is disposed in at least one of the plurality of base stations.

As Claim 10 depends from Claim 9, the arguments above with regard to the patentability of Claim 9 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 9, Examiner Dada interpreted the proxy server of Hsu as teaching the recited first controller. *See final Office Action, mailed December 31, 2007, page 4, section 6, fifth paragraph, first sentence.* In rejecting Claim 10, Examiner Dada stated that Hsu further teaches that the first controller is disposed in at least one of the plurality of base stations at column 6, lines 25-30.

*See final Office Action, page 5, section 7.* The cited passage is reproduced below:

Specifically, the IWF 18 provides an interworking function, where data packets transmitted by a digital telephone 16 and received by the BSC 14 are routed to the IWF 18 via the MSC 12 based on dialed digits supplied from the digital telephone 16.

The Appellants note that the cited passage makes no reference at all to the proxy server that Examiner Dada asserted describes the recited first controller. Furthermore, the Appellants are unable to find in the cited passage (or any other part of Hsu) any description of the proxy server of Hsu being disposed in the base station of Hsu.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 10 under § 103 be withdrawn and that Claim 10 be passed to allowance.

**O. CLAIM 11**

Claim 11 recites the wireless network of Claim 9, wherein the first controller is disposed in a mobile switching center of the wireless network.



As Claim 11 depends from Claim 9, the arguments above with regard to the patentability of Claim 9 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 9, Examiner Dada interpreted the proxy server of Hsu as teaching the recited first controller. *See final Office Action, mailed December 31, 2007, page 3, section 5, second paragraph, first sentence.* In rejecting Claim 11, Examiner Dada stated that Hsu further teaches that the first controller is disposed in at least one of the plurality of base stations at column 6, lines 25-30. *See final Office Action, page 5, section 8.* The cited passage is reproduced below:

Specifically, the IWF 18 provides an interworking function, where data packets transmitted by a digital telephone 16 and received by the BSC 14 are routed to the IWF 18 via the MSC 12 based on dialed digits supplied from the digital telephone 16.

The Appellants note that the cited passage makes no reference at all to the proxy server that Examiner Dada asserted describes the recited first controller. Furthermore, the Appellants are unable to find in the cited passage (or any other part of Hsu) any description of the proxy server of Hsu being disposed in the mobile switching center of Hsu.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 11 under § 103 be withdrawn and that Claim 11 be passed to allowance.

**P.     CLAIM 12**

Claim 12 recites the wireless network of Claim 9, further comprising a second controller capable of determining that said unprovisioned mobile station is unprovisioned.

As Claim 12 depends from Claim 9, the arguments above with regard to the patentability of Claim 9 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 12, Examiner Dada makes the conclusory statement, "As per claim [12], Hsu further teaches determining the unprovisioned mobile stations is (sic) unprovisioned (column 15, lines 7-10 and 21-25)." *Final Office Action, mailed December 31, 2007, page 5, section 9.*

Initially, the Appellants note that Examiner Dada has failed even to assert that Hsu or Applegate describes or suggests a second controller. As such, the Examiner has failed to establish a *prima facie* case of obviousness by failing to show that the prior art teaches or suggests all the elements of the claim.

The cited passages state:

As shown in FIG. 4B , the digital telephone 16 then establishes an initial two-way application session 62 with the proxy server 20 in step 128 . The digital telephone 16 also sends a data activation request with a security key and an international mobile station identity (IMSI). *Hsu, col. 15, lines 7-11.*

The proxy gateway 20 will also access the database [28] to determine if the user is in the active mode, indicating that the subscriber is already activated. If the user is not in an active mode, the proxy server 20 accepts the provisioning request in step 134 by transmitting a uniform resource locator (URL) to the digital telephone 16 and initiates a secure link using the user authenticated code and a public key encryption algorithm, such as the Diffie-Hellman algorithm. *Hsu, col. 15, lines 21-29. Reference character typo corrected.*

In rejecting Claim 9, Examiner Dada interpreted the proxy server of Hsu as teaching the recited first controller. *See final Office Action, mailed December 31, 2007, page 3, section 5, second paragraph, first sentence.* The passages cited in rejecting Claim 12 provide further description of the proxy server and, therefore, do not describe the second controller recited in Claim 12.

As such, the Appellants submit that Examiner Dada has failed to fully and clearly state the grounds for rejecting Claim 12. Specifically, the Examiner has not shown where Hsu describes the recited second controller capable of determining that an unprovisioned mobile station is unprovisioned.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 12 under § 103 be withdrawn and that Claim 12 be passed to allowance.

**Q.     CLAIM 13**

Claim 13 recites the security device of Claim 12, wherein the second controller determines that the unprovisioned mobile station is unprovisioned if the unprovisioned mobile station is unable to authenticate to the wireless network.

As Claim 13 depends from Claim 12, the arguments above with regard to the patentability of Claim 12 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 13, Examiner Dada makes the conclusory statement, “As per claim [13], Hsu further teaches determining the unprovisioned mobile stations is (sic) unprovisioned (column 15, lines 7-10 and 21-25).” *Final Office Action, mailed December 31, 2007, page 5, section 9.*

Initially, the Appellants note that Examiner Dada has failed even to assert that Hsu or Applegate describes or suggests determining that a mobile station is unprovisioned from the inability of the mobile station to authenticate to a wireless network. As such, the Examiner has failed to

establish a *prima facie* case of obviousness by failing to show that the prior art teaches or suggests all the elements of the claim.

The cited passages state:

As shown in FIG. 4B , the digital telephone 16 then establishes an initial two-way application session 62 with the proxy server 20 in step 128 . The digital telephone 16 also sends a data activation request with a security key and an international mobile station identity (IMSI). *Hsu, col. 15, lines 7-11.*

The proxy gateway 20 will also access the database [28] to determine if the user is in the active mode, indicating that the subscriber is already activated. If the user is not in an active mode, the proxy server 20 accepts the provisioning request in step 134 by transmitting a uniform resource locator (URL) to the digital telephone 16 and initiates a secure link using the user authenticated code and a public key encryption algorithm, such as the Diffie-Hellman algorithm. *Hsu, col. 15, lines 21-29. Reference character typo corrected.*

The Appellants are unable to find in the cited passages any teaching or suggestion of a mobile station authenticating to a wireless network, much less determining that a mobile station is unprovisioned from its inability to authenticate to the network.

As such, the Appellants submit that Examiner Dada has failed to fully and clearly state the grounds for rejecting Claim 13. Specifically, the Examiner has not shown where Hsu describes the recited second controller capable of determining that an unprovisioned mobile station is unprovisioned if the mobile station is unable to authenticate to the wireless network.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 13 under § 103 be withdrawn and that Claim 13 be passed to allowance.

**R.     CLAIM 14**

Claim 14 recites the security device of Claim 12, wherein the second controller determines that the unprovisioned mobile station is unprovisioned according to a predetermined telephone number associated with a service provisioning process selected by the unprovisioned mobile station.

As Claim 14 depends from Claim 12, the arguments above with regard to the patentability of Claim 12 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 14, Examiner Dada makes the conclusory statement, “As per claim [14], Hsu further teaches determining the unprovisioned mobile stations is (sic) unprovisioned (column 15, lines 7-10 and 21-25).” *Final Office Action, mailed December 31, 2007, page 5, section 9.*

Initially, the Appellants note that Examiner Dada has failed even to assert that Hsu or Applegate describes or suggests determining that a mobile station is unprovisioned according to a predetermined telephone number associated with a service provisioning process selected by the unprovisioned mobile station. As such, the Examiner has failed to establish a *prima facie* case of obviousness by failing to show that the prior art teaches or suggests all the elements of the claim.

The cited passages state:

As shown in FIG. 4B , the digital telephone 16 then establishes an initial two-way application session 62 with the proxy server 20 in step 128 . The digital telephone 16 also sends a data activation request with a security key and an international mobile station identity (IMSI). *Hsu, col. 15, lines 7-11.*

The proxy gateway 20 will also access the database [28] to determine if the user is in the active mode, indicating that the subscriber is already activated. If the user is not in an active mode, the proxy server 20 accepts the provisioning request in step 134 by transmitting a uniform resource locator (URL) to the digital telephone 16 and initiates a secure link using the user authenticated code and a public key encryption

algorithm, such as the Diffie-Hellman algorithm. *Hsu, col. 15, lines 21-29. Reference character typo corrected.*

The Appellants are unable to find in the cited passages any teaching or suggestion of predetermined telephone numbers associated with a service provisioning process, or an unprovisioned mobile station selecting a service provisioning process, much less determining that a mobile station is unprovisioned according to a predetermined telephone number associated with a service provisioning process selected by the unprovisioned mobile station

As such, the Appellants submit that Examiner Dada has failed to fully and clearly state the grounds for rejecting Claim 14. Specifically, the Examiner has not shown where Hsu describes the recited second controller capable of determining that an unprovisioned mobile station is unprovisioned according to a predetermined telephone number associated with a service provisioning process selected by the unprovisioned mobile station.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 14 under § 103 be withdrawn and that Claim 14 be passed to allowance.

S. CLAIM 15

Claim 15 recites the security device of Claim 12, wherein the second controller determines that the unprovisioned mobile station is unprovisioned according to data retrieved from a home location register associated with said wireless network.

As Claim 15 depends from Claim 12, the arguments above with regard to the patentability of Claim 12 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 15, Examiner Dada makes the conclusory statement, "As per claim [15], Hsu further teaches determining the unprovisioned mobile stations is (sic) unprovisioned (column 15, lines 7-10 and 21-25)." *Final Office Action, mailed December 31, 2007, page 5, section 9.*

Initially, the Appellants note that Examiner Dada has failed even to assert that Hsu or Applegate describes or suggests determining that a mobile station is unprovisioned according to data retrieved from a home location register associated with said wireless network. As such, the Examiner has failed to establish a *prima facie* case of obviousness by failing to show that the prior art teaches or suggests all the elements of the claim.

The cited passages state:

As shown in FIG. 4B , the digital telephone 16 then establishes an initial two-way application session 62 with the proxy server 20 in step 128 . The digital telephone 16 also sends a data activation request with a security key and an international mobile station identity (IMSI). *Hsu, col. 15, lines 7-11.*

The proxy gateway 20 will also access the database [28] to determine if the user is in the active mode, indicating that the subscriber is already activated. If the user is not in an active mode, the proxy server 20 accepts the provisioning request in step 134 by transmitting a uniform resource locator (URL) to the digital telephone 16 and initiates a secure link using the user authenticated code and a public key encryption

algorithm, such as the Diffie-Hellman algorithm. *Hsu, col. 15, lines 21-29. Reference character typo corrected.*

The Appellants are unable to find in the cited passages any teaching or suggestion of determining that a mobile station is unprovisioned according to data retrieved from a home location register associated with said wireless network.

The user database 28 described in the cited passages stores an international mobile station identify (IMSI), a security key, and an 'active' status mode indication. *See Hsu, col. 15, lines 13-29, and Claims 6, 24 and 33.* The user database 28 is clearly not a home location register.

In fact, Hsu describes a home location register as separate from the user database 28. The home location register is part of operation maintenance provisioning system 44. *See Hsu, Fig. 1, col. 7, lines 50-59.*

As such, the Appellants submit that Examiner Dada has failed to fully and clearly state the grounds for rejecting Claim 15. Specifically, the Examiner has not shown where Hsu describes the recited second controller capable of determining that an unprovisioned mobile station is unprovisioned according to data retrieved from a home location register associated with said wireless network.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 15 under § 103 be withdrawn and that Claim 15 be passed to allowance.



**T. CLAIM 16**

Claim 16 recites the security device of Claim 9, wherein the first controller selects the at least one provisioning server by selecting said IP address in said replacement IP packet header according to a load spreading algorithm.

As Claim 16 depends from Claim 9, the arguments above with regard to the patentability of Claim 9 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 16, Examiner Dada stated that Applegate describes selecting an IP address according to a load sharing algorithm in column 5, lines 34-65. *See final Office Action, mailed December 31, 2007, page 5, section 10.* The Appellants respectfully submit that Examiner Dada appears to mischaracterize the teaching of the Applegate reference.

The cited passage is reproduced below:

The message packet is then passed along 366 to TCP/IP 226. The modified message packet has: source IP address 199.198.10.2, source port 1024, destination IP address 199.198.10.1, and destination port 21. The IP layer then examines the IP header, determines that the message is destined for the Firewall machine and accepts it. TCP/IP passes the message along to the FTP proxy, which is listening for incoming messages. The FTP proxy 310 obtains the message, verifies that the FTP connection is permitted by an access control entry, and hides the internal source of the message from the external network. *Applegate, col. 5, lines 34-64*

There is clearly no description in the cited passage of selecting an IP address according to a load sharing algorithm, as asserted by Examiner Dada. In fact, Applegate describes a firewall that reroutes an FTP packet to a local FTP proxy by replacing the IP address of an external FTP server with the IP address of the FTP proxy. There is only a single FTP proxy in Applegate, therefore

Applegate cannot teach selecting one of a plurality of servers, much less selecting a server according to a load sharing algorithm.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 16 under § 103 be withdrawn and that Claim 16 be passed to allowance.

U.     CLAIM 17

Claim 17 recites a method for use in a wireless network comprising a plurality of base stations, each of the base stations capable of communicating with a plurality of mobile stations. The method prevents an unprovisioned one of the plurality of mobile stations from accessing an Internet protocol (IP) data network through the wireless network and comprises the steps of:

- receiving from the unprovisioned mobile station an IP data packet comprising an IP packet header and an IP packet payload;
- determining that the unprovisioned mobile station is unprovisioned; and
- replacing the IP packet header with a replacement IP packet header comprising an IP address of a selected one of a plurality of provisioning servers associated with the wireless network.

First, Examiner Dada acknowledges that Hsu does not describe a controller that receives an IP data packet and replaces the received IP packet header with an IP packet header including an IP address of a selected one of a plurality of provisioning servers. But, Examiner Dada asserts that replacing an IP header with the IP address of a server is well-known in the art, “in order to route data to a correct destination address and further provide efficient data transmission.” *See final Office Action, mailed December 31, 2007, sentence beginning last line of page 3.*

However, routing data to a correct destination address and providing efficient data transmission are problems that Hsu has already solved. Hsu ensures that provisioning messages go only to the provisioning server by providing the server's address to a wireless device for its use during provisioning. As such Hsu has provided a mechanism for routing data to a correct destination address and providing efficient data transmission. Examiner Dada has provided no explanation why a person of ordinary skill in the art having common sense at the time of the invention would have reasonably looked to Applegate to solve a problem already solved by Hsu. Instead, the Appellants respectfully submit that Examiner Dada has impermissibly used Claim 1 as a guide in formulating the rejection.

Second, in further support of the assertion that replacing an IP header with the IP address of a server is well-known in the art, Examiner Dada cites Applegate. The Examiner asserts that Applegate describes replacing an IP packet header with a replacement IP packet header including the IP address of a selected one of a plurality of servers associated with a wireless network, citing column 5, lines 34-65. The Applicants respectfully submit that Examiner Dada appears to mischaracterize several aspects of the Applegate reference.

Applegate describes a firewall that reroutes an FTP packet to a local FTP proxy by replacing the IP address of an external FTP server with the IP address of the FTP proxy. However, Applegate makes no mention of a plurality of FTP proxies, nor of selecting one proxy from a plurality of proxies. Also, Applegate describes a communication security system that uses a server to communicate to an unprotected network, such as the Internet, but Applegate makes no mention of a

wireless network. Furthermore, Examiner Dada asserts that a person of skill in the art would turn to the teaching of Applegate in order to efficiently route packets and further enhance security of the system. Applegate provides no suggestion that replacing the IP address of an FTP server with the address of an FTP proxy provides efficient routing of packets, and the security enhancements of Applegate come not from replacing the IP address in the FTP packet, but rather from checking in the FTP proxy whether a connection to the intended FTP server is permitted.

In short, Examiner Dada has suggested that a person of skill in the art would combine Hsu and Applegate to solve a problem that does not exist in Hsu with a feature of Applegate that does not provide the improvement that the Examiner suggests. The suggestion that the security of over-the-air provisioning should be improved and the solution of replacing the IP address in a data packet from an unprovisioned mobile station with the IP address of a provisioning server come only from the present application, not from the cited references.

Third, while Hsu describes a proxy gateway sending the URL of a provisioning server to a wireless device, Hsu describes only a single provisioning server, not a plurality of provisioning servers, as asserted by Examiner Dada.

As such, Examiner Dada has not shown that the cited references teach or suggest all the limitations of Claim 17. For these reasons, the Examiner has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 17 under § 103 be withdrawn and that Claim 17 be passed to allowance.

V. CLAIM 18

Claim 18 recites the security device of Claim 17, wherein the step of determining comprises the step of determining that the unprovisioned mobile station is unable to authenticate to the wireless network.

As Claim 18 depends from Claim 17, the arguments above with regard to the patentability of Claim 17 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 17, Examiner Dada makes the conclusory statement, "As per claim [17], Hsu further teaches determining the unprovisioned mobile stations is (sic) unprovisioned (column 15, lines 7-10 and 21-25)." *Final Office Action, mailed December 31, 2007, page 5, section 9.*

Initially, the Appellants note that Examiner Dada has failed even to assert that Hsu or Applegate describes or suggests determining that a mobile station is unprovisioned by determining the inability of the mobile station to authenticate to a wireless network. As such, the Examiner has failed to establish a *prima facie* case of obviousness by failing to show that the prior art teaches or suggests all the elements of the claim.

The cited passages state:

As shown in FIG. 4B, the digital telephone 16 then establishes an initial two-way application session 62 with the proxy server 20 in step 128. The digital telephone 16 also sends a data activation request with a security key and an international mobile station identity (IMSI). *Hsu, col. 15, lines 7-11.*

The proxy gateway 20 will also access the database [28] to determine if the user is in the active mode, indicating that the subscriber is already activated. If the user is not in an active mode, the proxy server 20 accepts the provisioning request in step 134 by transmitting a uniform resource locator (URL) to the digital telephone 16 and initiates a secure link using the user authenticated code and a public key encryption

algorithm, such as the Diffie-Hellman algorithm. *Hsu, col. 15, lines 21-29. Reference character typo corrected.*

The Appellants are unable to find in the cited passages any teaching or suggestion of a mobile station authenticating to a wireless network, much less determining that a mobile station is unprovisioned from its inability to authenticate to the network.

As such, the Appellants submit that Examiner Dada has failed to fully and clearly state the grounds for rejecting Claim 18. Specifically, the Examiner has not shown where Hsu describes the recited step of determining that an unprovisioned mobile station is unprovisioned by determining if the mobile station is unable to authenticate to the wireless network.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 18 under § 103 be withdrawn and that Claim 18 be passed to allowance.

**W. CLAIM 19**

Claim 19 recites the security device of Claim 17, wherein the step of determining comprises the step of determining that the unprovisioned mobile station selected a predetermined telephone number associated with a service provisioning process.

As Claim 19 depends from Claim 17, the arguments above with regard to the patentability of Claim 17 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 19, Examiner Dada makes the conclusory statement, "As per claim [19], Hsu further teaches determining the unprovisioned mobile stations is (sic) unprovisioned (column 15, lines 7-10 and 21-25)." *Final Office Action, mailed December 31, 2007, page 5, section 9.*

Initially, the Appellants note that Examiner Dada has failed even to assert that Hsu or Applegate describes or suggests determining that a mobile station is unprovisioned by determining that the mobile station selected a predetermined telephone number associated with a service provisioning process. As such, the Examiner has failed to establish a *prima facie* case of obviousness by failing to show that the prior art teaches or suggests all the elements of the claim.

The cited passages state:

As shown in FIG. 4B, the digital telephone 16 then establishes an initial two-way application session 62 with the proxy server 20 in step 128. The digital telephone 16 also sends a data activation request with a security key and an international mobile station identity (IMSI). *Hsu, col. 15, lines 7-11.*

The proxy gateway 20 will also access the database [28] to determine if the user is in the active mode, indicating that the subscriber is already activated. If the user is not in an active mode, the proxy server 20 accepts the provisioning request in step 134 by transmitting a uniform resource locator (URL) to the digital telephone 16 and initiates a secure link using the user authenticated code and a public key encryption algorithm, such as the Diffie-Hellman algorithm. *Hsu, col. 15, lines 21-29. Reference character typo corrected.*

The Appellants are unable to find in the cited passages any teaching or suggestion of predetermined telephone numbers associated with a service provisioning process, or an unprovisioned mobile station selecting a service provisioning process, much less determining that a mobile station is unprovisioned by determining that the mobile station selected a predetermined telephone number associated with a service provisioning process.

As such, the Appellants submit that Examiner Dada has failed to fully and clearly state the grounds for rejecting Claim 19. Specifically, the Examiner has not shown where Hsu describes the recited second controller capable of determining that an unprovisioned mobile station is unprovisioned by determining that the mobile station selected a predetermined telephone number associated with a service provisioning process.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 19 under § 103 be withdrawn and that Claim 19 be passed to allowance.

**X. CLAIM 20**

Claim 20 recites the security device of Claim 17, wherein the step of determining that the unprovisioned mobile station is unprovisioned comprises the step of examining data retrieved from a home location register associated with the wireless network.

As Claim 20 depends from Claim 17, the arguments above with regard to the patentability of Claim 17 over Hsu and Applegate apply here as well, and are incorporated herein by reference.

In rejecting Claim 20, Examiner Dada makes the conclusory statement, “As per claim [20], Hsu further teaches determining the unprovisioned mobile stations is (sic) unprovisioned (column 15, lines 7-10 and 21-25).” *Final Office Action, mailed December 31, 2007, page 5, section 9.*

Initially, the Appellants note that Examiner Dada has failed even to assert that Hsu or Applegate describes or suggests determining that a mobile station is unprovisioned by examining



data retrieved from a home location register associated with the wireless network. As such, the Examiner has failed to establish a *prima facie* case of obviousness by failing to show that the prior art teaches or suggests all the elements of the claim.

The cited passages state:

As shown in FIG. 4B , the digital telephone 16 then establishes an initial two-way application session 62 with the proxy server 20 in step 128 . The digital telephone 16 also sends a data activation request with a security key and an international mobile station identity (IMSI). *Hsu, col. 15, lines 7-11.*

The proxy gateway 20 will also access the database [28] to determine if the user is in the active mode, indicating that the subscriber is already activated. If the user is not in an active mode, the proxy server 20 accepts the provisioning request in step 134 by transmitting a uniform resource locator (URL) to the digital telephone 16 and initiates a secure link using the user authenticated code and a public key encryption algorithm, such as the Diffie-Hellman algorithm. *Hsu, col. 15, lines 21-29. Reference character typo corrected.*

The Appellants are unable to find in the cited passages any teaching or suggestion of determining that a mobile station is unprovisioned by examining data retrieved from a home location register associated with the wireless network.

The user database 28 described in the cited passages stores an international mobile station identify (IMSI), a security key, and an 'active' status mode indication. *See Hsu, col. 15, lines 13-29, and Claims 6, 24 and 33.* The user database 28 is clearly not a home location register.

In fact, Hsu describes a home location register as separate from the user database 28. The home location register is part of operation maintenance provisioning system 44. *See Hsu, Fig. 1, col. 7, lines 50-59.*

As such, the Appellants submit that Examiner Dada has failed to fully and clearly state the grounds for rejecting Claim 20. Specifically, the Examiner has not shown where Hsu describes the recited second controller capable of determining that an unprovisioned mobile station is unprovisioned by examining data retrieved from a home location register associated with the wireless network.

For these reasons, Examiner Dada has failed to establish a *prima facie* case of obviousness. Accordingly, the Appellants respectfully request that the final rejection of Claim 20 under § 103 be withdrawn and that Claim 20 be passed to allowance.

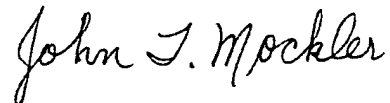
**SUMMARY**

For the reasons given above, the Appellants respectfully request reconsideration and allowance of pending claims and that this Application be passed to issue. If any outstanding issues remain, or if the Examiner has any further suggestions for expediting allowance of this Application, the Appellants respectfully invite the Examiner to contact the undersigned at the telephone number indicated below or at *[jmockler@munckcarter.com](mailto:jmockler@munckcarter.com)*.

The Commissioner is hereby authorized to charge any additional fees connected with this communication or credit any overpayment to Deposit Account No. 50-0208.

Respectfully submitted,

MUNCK CARTER, P.C.



Date: June 6, 2008

P.O. Drawer 800889  
Dallas, Texas 75380  
Phone: (972) 628-3600  
Fax: (972) 628-3616  
E-mail: *[jmockler@munckcarter.com](mailto:jmockler@munckcarter.com)*

\_\_\_\_\_  
John T. Mockler  
Registration No. 39,775

**APPENDIX A**  
**CLAIMS APPENDIX**

The status of the claims is as follows:

1. (Previously Presented) For use in a wireless network comprising a plurality of base stations, each of said base stations capable of communicating with a plurality of mobile stations, a security device capable of preventing an unprovisioned one of said plurality of mobile stations from accessing an Internet protocol (IP) data network through said wireless network, said security device comprising:

a first controller capable of receiving from said unprovisioned mobile station an IP data packet comprising an IP packet header and an IP packet payload and replacing said IP packet header with a replacement IP packet header comprising an IP address of a selected one of a plurality of provisioning servers associated with said wireless network.

2. (Original) The security device set forth in Claim 1 wherein said first controller is disposed in at least one of said plurality of base stations.

3. (Original) The security device set forth in Claim 1 wherein said first controller is disposed in a mobile switching center of said wireless network.

4. (Original) The security device set forth in Claim 1 further comprising a second controller capable of determining that said unprovisioned mobile station is unprovisioned.

5. (Previously Presented) The security device set forth in Claim 4 wherein said second controller determines that said unprovisioned mobile station is unprovisioned if said unprovisioned mobile station is unable to authenticate to said wireless network.

6. (Previously Presented) The security device set forth in Claim 4 wherein said second controller determines that said unprovisioned mobile station is unprovisioned according to a predetermined telephone number associated with a service provisioning process selected by said unprovisioned mobile station.

7. (Previously Presented) The security device set forth in Claim 4 wherein said second controller determines that said unprovisioned mobile station is unprovisioned according to data retrieved from a home location register associated with said wireless network.

8. (Original) The security device set forth in Claim 1 wherein said first controller selects said least one provisioning server by selecting said IP address in said replacement IP packet header according to a load spreading algorithm.

9. (Previously Presented) A wireless network comprising:
- a plurality of base stations, each of said base stations capable of communicating with a plurality of mobile stations;
  - at least one provisioning server; and
  - a security device capable of preventing an unprovisioned one of said plurality of mobile stations from accessing an Internet protocol (IP) data network through said wireless network, said security device comprising:
    - a first controller capable of receiving from said unprovisioned mobile station an IP data packet comprising an IP packet header and an IP packet payload and replacing said IP packet header with a replacement IP packet header comprising an IP address of said provisioning server.
10. (Original) The wireless network set forth in Claim 9 wherein said first controller is disposed in at least one of said plurality of base stations.
11. (Original) The wireless network set forth in Claim 9 wherein said first controller is disposed in a mobile switching center of said wireless network.
12. (Original) The wireless network set forth in Claim 9 further comprising a second controller capable of determining that said unprovisioned mobile station is unprovisioned.

13. (Previously Presented) The wireless network set forth in Claim 12 wherein said second controller determines that said unprovisioned mobile station is unprovisioned if said unprovisioned mobile station is unable to authenticate to said wireless network.

14. (Previously Presented) The wireless network set forth in Claim 12 wherein said second controller determines that said unprovisioned mobile station is unprovisioned according to a predetermined telephone number associated with a service provisioning process selected by said unprovisioned mobile station.

15. (Previously Presented) The wireless network set forth in Claim 12 wherein said second controller determines that said unprovisioned mobile station is unprovisioned according to data retrieved from a home location register associated with said wireless network.

16. (Original) The wireless network set forth in Claim 9 wherein said first controller selects said least one provisioning server by selecting said IP address in said replacement IP packet header according to a load spreading algorithm.

17. (Previously Presented) For use in a wireless network comprising a plurality of base stations, each of the base stations capable of communicating with a plurality of mobile stations, a method of preventing an unprovisioned one of the plurality of mobile stations from accessing an Internet protocol (IP) data network through the wireless network, the method comprising the steps of:

receiving from the unprovisioned mobile station an IP data packet comprising an IP packet header and an IP packet payload;

determining that the unprovisioned mobile station is unprovisioned; and

replacing the IP packet header with a replacement IP packet header comprising an IP address of a selected one of a plurality of provisioning servers associated with the wireless network.

18. (Original) The method set forth in Claim 17 wherein the step of determining comprises the step of determining that the unprovisioned mobile station is unable to authenticate to the wireless network.

19. (Original) The method set forth in Claim 17 wherein the step of determining comprises the step of determining that the unprovisioned mobile station selected a predetermined telephone number associated with a service provisioning process.



20. (Original) The method set forth in Claim 17 wherein the step of determining that the unprovisioned mobile station is unprovisioned comprises the step of examining data retrieved from a home location register associated with the wireless network.

**APPENDIX B**  
**EVIDENCE APPENDIX**

None. No evidence has been submitted pursuant to 37 CFR 1.130, 1.131, or 1.132, nor is there any other evidence entered by the examiner and relied upon by appellant in the appeal.

**APPENDIX C**  
**RELATED PROCEEDINGS APPENDIX**

None. To the best knowledge and belief of the undersigned attorney, there are no decisions rendered by a court or the Board in any proceeding identified pursuant to 37 CFR 41.37(c)(1)(ii).